



**ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ
КИБЕРНЕТИЧЕСКИХ СИСТЕМ**

**Кафедра
«Криптология и кибербезопасность»**

Контрольная работа №1

«Поиск уязвимостей по открытым источникам»

Исполнитель:

студент гр. Б19-515

Щербакова А. Е.

подпись,

дата

Преподаватель:

Анисимов Д.В.

подпись,

дата

Москва — 2023

1 Введение

Для анализа уязвимостей выбраны следующие пакеты: sudo 1.8.20 и Perl 5.26.3. Для поиска уязвимостей использовался сайт <https://nvd.nist.gov/products/cpe/search>

2 Пакет sudo 1.8.20

Найдено 10 уязвимостей: CVE-2023-22809, CVE-2022-43995, CVE-2021-3156, CVE-2021-23240, CVE-2021-23239, CVE-2019-18634, CVE-2019-18684, CVE-2019-14287, CVE-2017-1000368, CVE-2017-1000367.

nvd.nist.gov

NVD - Results

Q Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

There are 10 matching records.
Displaying matches 1 through 10.

- Results Type: Overview
- Keyword (text search):
cpe:2.3:a:sudo_project:sudo:1.8.20:*:*:*:*:*
- CPE Name Search: true

Vuln ID	Summary	CVSS Severity
CVE-2023-22809	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user-specified editor may contain a "--" argument that defeats a protection mechanism, e.g., an EDITOR='vim -- /path/to/extra/file' value. Published: января 18, 2023; 12:15:10 PM -0500	V3.1: 7.5 HIGH V2.0:(not available)
CVE-2022-43995	Sudo 1.8.0 through 1.9.12, with the crypt() password backend, contains a plugins/sudoers/auth/passwd.c array-out-of-bounds error that can result in a heap-based buffer over-read. This can be triggered by arbitrary local users with access to Sudo by entering a password of seven characters or fewer. The impact could vary depending on the system libraries, compiler, and processor architecture. Published: ноября 02, 2022; 10:15:16 AM -0400	V3.1: 7.1 HIGH V2.0:(not available)
CVE-2021-3156	Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character. Published: января 26, 2021; 4:15:12 PM -0500	V3.1: 7.5 HIGH V2.0: 7.2 HIGH
CVE-2021-23240	selinux_edit_copy_tfiles in sudoedit in Sudo before 1.9.5 allows a local unprivileged user to gain file ownership and escalate privileges by replacing a temporary file with a symlink to an arbitrary file target. This affects SELinux RBAC support in permissive mode. Machines without SELinux are not vulnerable. Published: января 12, 2021; 4:15:14 AM -0500	V3.1: 7.5 HIGH V2.0: 4.4 MEDIUM
CVE-2021-23239	The sudoedit personality of Sudo before 1.9.5 may allow a local unprivileged user to perform arbitrary directory-existence tests by winning a	V3.1: 2.5 LOW

Рисунок 1 – Уязвимости пакета sudo 1.8.20 (часть 1)

nvd.nist.gov			
NVD - Results			
Published: января 12, 2021; 4:15:14 AM -0500			
CVE-2021-23239	The sudoedit personality of Sudo before 1.9.5 may allow a local unprivileged user to perform arbitrary directory-existence tests by winning a sudo_edit.c race condition in replacing a user-controlled directory by a symlink to an arbitrary path.	V3.1: 2.5 LOW V2.0: 1.9 LOW	
Published: января 12, 2021; 4:15:14 AM -0500			
CVE-2019-18634	In Sudo before 1.8.26, if pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process. (pwfeedback is a default setting in Linux Mint and elementary OS; however, it is NOT the default for upstream and many other packages, and would exist only if enabled by an administrator.) The attacker needs to deliver a long string to the stdin of getln() in tgetpass.c.	V3.1: 7.8 HIGH V2.0: 4.6 MEDIUM	
Published: января 29, 2020; 1:15:12 PM -0500			
CVE-2019-18684	** DISPUTED ** Sudo through 1.8.29 allows local users to escalate to root if they have write access to file descriptor 3 of the sudo process. This occurs because of a race condition between determining a uid, and the setresuid and openat system calls. The attacker can write "ALL ALL=(ALL) NOPASSWD:ALL" to /proc/####/fd/3 at a time when Sudo is prompting for a password. NOTE: This has been disputed due to the way Linux /proc works. It has been argued that writing to /proc/####/fd/3 would only be viable if you had permission to write to /etc/sudoers. Even with write permission to /proc/####/fd/3, it would not help you write to /etc/sudoers.	V3.1: 7.0 HIGH V2.0: 6.9 MEDIUM	
Published: ноября 04, 2019; 11:15:11 AM -0500			
CVE-2019-14287	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#\$(0xffffffff)" command.	V3.1: 8.8 HIGH V2.0: 9.0 HIGH	
Published: октября 17, 2019; 2:15:12 PM -0400			
CVE-2017-1000368	Todd Miller's sudo version 1.8.20p1 and earlier is vulnerable to an input validation (embedded newlines) in the get_process_ttyname() function resulting in information disclosure and command execution.	V3.0: 8.2 HIGH V2.0: 7.2 HIGH	
Published: июня 05, 2017; 12:29:00 PM -0400			
CVE-2017-1000367	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.	V3.0: 6.4 MEDIUM V2.0: 6.9 MEDIUM	
Published: июня 05, 2017; 10:29:00 AM -0400			

Рисунок 2 – Уязвимости пакета sudo 1.8.20 (часть 2)

Далее скриншотов по каждой уязвимости не приложено, так как их слишком много, а их содержание как раз и представлено в таблице.

Способ устранения для всех уязвимостей – обновиться до исправленной версии пакета.

Таблица 1 – Описание уязвимостей пакета sudo 1.8.20.

Название уязвимости	Описание и вектор атаки	Критичность	Устранение
CVE-2022-43995	Sudo с 1.8.0 по 1.9.12 с серверной частью пароля crypt() содержит ошибку plugins/sudoers/auth/passwd.c, выходящую за пределы массива, которая может привести к переполнению буфера на основе кучи. Это может быть вызвано произвольными локальными пользователями, имеющими доступ к Sudo, путем ввода пароля из семи символов или	CVSS 3.x – High (7.1) CVSS 2.0 – not available	Исправлена в версии sudo 1.8.29-4 и 1.9.13

	<p>менее. Влияние может варьироваться в зависимости от системных библиотек, компилятора и архитектуры процессора.</p>		
CVE-2021-3156	<p>Sudo до 1.9.5p2 содержит случайную ошибку, которая может привести к переполнению буфера на основе кучи, что позволяет повысить привилегии root с помощью "sudoedit -s" и аргумента командной строки, который заканчивается одним символом обратной косой черты.</p> <p>Эксплойт: https://github.com/worawit/CVE-2021-3156</p>	<p>CVSS 3.x – High (7.8) CVSS 2.0 – not available</p>	<p>Ошибка исправлена в sudo 1.8.32 и 1.9.5p2.</p>
CVE-2023-22809	<p>В Sudo до 1.9.12p2 функция sudoedit (она же -e) неправильно обрабатывает дополнительные аргументы, передаваемые в пользовательских переменных среды (SUDO_EDITOR, VISUAL и EDITOR), позволяя локальному злоумышленнику добавлять произвольные записи в список файлов для обработки. Это может привести к повышению привилегий. Затронутые версии - с 1.8.0 по 1.9.12.p1. Проблема существует из-за того, что указанный пользователем редактор может содержать аргумент "--", который отключает механизм защиты, например, значение EDITOR='vim -- /path/to/extra/file'.</p> <p>Эксплойт: https://github.com/M4fiaB0y/CVE-2023-22809</p>	<p>CVSS 3.x – High (7.8) CVSS 2.0 – High (7.2)</p>	<p>Исправлена в версии sudo 1.9.12p2</p>

CVE-2021-23240	selinux_edit_copy_tfiles в sudoedit в Sudo до версии 1.9.5 позволяет локальному непривилегированному пользователю получить право собственности на файл и повысить привилегии, заменив временный файл символической ссылкой на произвольный целевой файл. Это влияет на поддержку SELinux RBAC в разрешающем режиме. Машины без SELinux не уязвимы.	CVSS 3.x – High (7.8) CVSS 2.0 – Medium (4.4)	Исправлена в версии sudo 1.9.5
CVE-2021-23239	Идентификатор sudoedit в Sudo до версии 1.9.5 может позволить локальному непривилегированному пользователю выполнять тесты на существование произвольного каталога, выиграв условие гонки sudo_edit.c при замене каталога, контролируемого пользователем, символической ссылкой на произвольный путь.	CVSS 3.x – Low (2.5) CVSS 2.0 – Low (1.9)	Исправлена в версии sudo 1.9.5
CVE-2019-18634	В Sudo до версии 1.8.26, если pwfeedback включен в /etc/sudoers, пользователи могут вызвать переполнение буфера на основе стека в привилегированном процессе sudo. (pwfeedback - это настройка по умолчанию в Linux Mint и elementary OS; однако она не используется по умолчанию для upstream и многих других пакетов и будет существовать только в том случае, если включена администратором.) Злоумышленнику необходимо передать длинную строку в	CVSS 3.x – High (7.8) CVSS 2.0 – Medium (4.6)	Исправлена в версии sudo 1.8.26

	<p>stdin функции getting() в tgetpass.c.</p> <p>Эксплойт:</p> <p>https://github.com/Plazmaz/CVE-2019-18634</p>		
CVE-2019-18684	<p>Sudo до 1.8.29 позволяет локальным пользователям перейти на root, если у них есть доступ на запись к файловому дескриптору 3 процесса sudo. Это происходит из-за состояния гонки между определением uid и setresuid и open при системных вызовах. Злоумышленник может записать "ALL ALL=(ALL) NOPASSWD:ALL" в /proc/#####/fd/3 в то время, когда Sudo запрашивает пароль. ПРИМЕЧАНИЕ: Это было оспорено из-за того, как работает Linux / proc. Утверждалось, что запись в /proc /#####/fd/3 была бы жизнеспособной только в том случае, если бы у вас было разрешение на запись в /etc /sudoers. Даже с разрешением на запись в /proc /#####/fd /3 это не помогло бы вам записывать в /etc/sudoers.</p>	<p>CVSS 3.x – High (7.0)</p> <p>CVSS 2.0 – Medium (6.9)</p>	Исправлена в версии sudo 1.8.29
CVE-2019-14287	<p>В Sudo до версии 1.8.28 злоумышленник, имеющий доступ к учетной записи Runas ALL sudoer, может обойти определенные черные списки политик и модули PAM сеанса и вызвать неправильное ведение журнала, вызвав sudo с созданным идентификатором пользователя. Например, это позволяет обходить !root configuration и USER= logging для команды "sudo -u \#\$(0xffffffff)".</p>	<p>CVSS 3.x – High (8.8)</p> <p>CVSS 2.0 – High (9.0)</p>	Исправлена в версии sudo 1.8.28

	Эксплойт: https://www.sudo.ws/security/advisories/minus_1_uid/		
CVE-2017-1000368	Sudo Тодда Миллера версии 1.8.20p1 и более ранних уязвим для проверки ввода (встроенные новые строки) в функции <code>get_process_ttyname()</code> , что приводит к раскрытию информации и выполнению команды.	CVSS 3.x – High (8.2) CVSS 2.0 – High (7.2)	Исправлена в версии sudo 1.8.20p2
CVE-2017-1000367	Sudo от Тодда Миллера версии 1.8.20 и более ранних версий уязвим для проверки входных данных (встроенные пробелы) в функции <code>get_process_ttyname()</code> , что приводит к раскрытию информации и выполнению команды.	CVSS 3.x – Medium (6.4) CVSS 2.0 – Medium (6.9)	Исправлена в версии sudo 1.8.20p2

2 Пакет Perl 5.26.3

Найдено 9 уязвимостей: CVE-2021-36770, CVE-2020-12723, CVE-2020-10878, CVE-2016-1246, CVE-2011-3599, CVE-2011-2201, CVE-2010-1168, CVE-2009-1884, CVE-2009-0663.

nvd.nist.gov

NVD - Results

А

Q

Search Results

(Refine Search)

Sort results by:

Publish Date Descending

Sort

Search Parameters:

Results Type: Overview

Keyword (text search):
cpe:2.3:a:perl:perl:5.26.3:*:*:*:*:*

CPE Name Search: true

There are 9 matching records.
Displaying matches 1 through 9.

Vuln ID 基	Summary ⓘ	CVSS Severity ⓘ
CVE-2021-36770	Encode.pm, as distributed in Perl through 5.34.0, allows local users to gain privileges via a Trojan horse Encode::ConfigLocal library (in the current working directory) that preempts dynamic module loading. Exploitation requires an unusual configuration, and certain 2021 versions of Encode.pm (3.05 through 3.11). This issue occurs because the operator evaluates @INC in a scalar context, and thus @INC has only an integer value. Published: августа 11, 2021; 7:15:07 PM -0400	V3.1: 7.5 HIGH V2.0: 6.8 MEDIUM
CVE-2020-12723	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls. Published: июня 05, 2020; 11:15:10 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection. Published: июня 05, 2020; 10:15:10 AM -0400	V3.1: 8.6 HIGH V2.0: 7.5 HIGH
CVE-2016-1246	Buffer overflow in the DBD::mysql module before 4.037 for Perl allows context-dependent attackers to cause a denial of service (crash) via vectors related to an error message. Published: октября 05, 2016; 12:59:00 PM -0400	V3.0: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2011-3599	The Crypt::DSA (aka Crypt-DSA) module 1.17 and earlier for Perl, when /dev/random is absent, uses the Data::Random module, which makes it easier for remote attackers to spoof a signature, or determine the signing key of a signed message, via a brute-force attack. Published: октября 10, 2011; 6:55:06 AM -0400	V3.x:(not available) V2.0: 5.9 MEDIUM

Рисунок 3 – Уязвимости пакета Perl 5.26.3 (часть 1)

nvd.nist.gov

NVD - Results

🔍

🔖

CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection. Published: июня 05, 2020; 10:15:10 AM -0400	V3.1: 8.6 HIGH V2.0: 7.5 HIGH
CVE-2016-1246	Buffer overflow in the DBD::mysql module before 4.037 for Perl allows context-dependent attackers to cause a denial of service (crash) via vectors related to an error message. Published: октября 05, 2016; 12:59:00 PM -0400	V3.0: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2011-3599	The Crypt::DSA (aka Crypt-DSA) module 1.17 and earlier for Perl, when /dev/random is absent, uses the Data::Random module, which makes it easier for remote attackers to spoof a signature, or determine the signing key of a signed message, via a brute-force attack. Published: октября 10, 2011; 6:55:06 AM -0400	V3.x:(not available) V2.0: 5.8 MEDIUM
CVE-2011-2201	The Data::FormValidator module 4.66 and earlier for Perl, when untaint_all_constraints is enabled, does not properly preserve the taint attribute of data, which might allow remote attackers to bypass the taint protection mechanism via form input. Published: сентября 14, 2011; 12:05:23 PM -0400	V3.x:(not available) V2.0: 4.3 MEDIUM
CVE-2010-1168	The Safe (aka Safe.pm) module before 2.25 for Perl allows context-dependent attackers to bypass intended (1) Safe::reval and (2) Safe::rdo access restrictions, and inject and execute arbitrary code, via vectors involving implicitly called methods and implicitly blessed objects, as demonstrated by the (a) DESTROY and (b) AUTOLOAD methods, related to "automagic methods." Published: июня 21, 2010; 12:30:01 PM -0400	V3.x:(not available) V2.0: 7.5 HIGH
CVE-2009-1884	Off-by-one error in the bzip2 function in Bzip2.xs in the Compress-Raw-Bzip2 module before 2.018 for Perl allows context-dependent attackers to cause a denial of service (application hang or crash) via a crafted bzip2 compressed stream that triggers a buffer overflow, a related issue to CVE-2009-1391. Published: августа 19, 2009; 1:30:00 PM -0400	V3.x:(not available) V2.0: 4.3 MEDIUM
CVE-2009-0663	Heap-based buffer overflow in the DBD::Pg (aka DBD-Pg or libdbd-pg-perl) module 1.49 for Perl might allow context-dependent attackers to execute arbitrary code via unspecified input to an application that uses the getline and pg_getline functions to read database rows. Published: апреля 30, 2009; 4:30:00 PM -0400	V3.x:(not available) V2.0: 7.5 HIGH

Рисунок 4 – Уязвимости пакета sudo 5.26.3 (часть 1)

Таблица 2 – Описание уязвимостей пакета Perl 5.26.3.

Название уязвимости	Описание и вектор атаки	Критичность	Устранение
CVE-2021-36770	Encode.pm , распространяемый на Perl до версии 5.34.0, позволяет локальным пользователям получать привилегии с помощью троянского коня Encode::ConfigLocal library (в текущем рабочем каталоге), который предотвращает загрузку динамического модуля. Эксплуатация требует необычной конфигурации, и некоторые версии 2021 года Encode.pm (с 3.05 по 3.11). Эта проблема возникает из-за того, что оператор вычисляет @INC в скалярном контексте, и, таким образом, @INC имеет только целочисленное значение.	CVSS 3.x – High (7.8) CVSS 2.0 – Medium (6.8)	Исправлена в версии 5.34.0
CVE-2020-12723	regcomp.c в Perl до версии 5.30.3 допускает переполнение буфера с помощью созданного регулярного выражения из-за рекурсивных вызовов S_study_chunk.	CVSS 3.x – High (7.5) CVSS 2.0 – Medium (5.0)	Исправлена в версии 5.30.3
CVE-2020-10878	Perl до версии 5.30.3 имеет переполнение целых чисел, связанное с неправильным обращением с ситуацией "PL_regkind[OP(n)] == NOTHING". Созданное регулярное выражение может привести к искаженному байт-коду с возможностью внедрения команд.	CVSS 3.x – High (7.5) CVSS 2.0 – High (8.6)	Исправлена в версии 5.30.3
CVE-2016-1246	Переполнение буфера в модуле DBD::mysql до версии 4.037 для Perl позволяет контекстно-зависимым злоумышленникам вызывать	CVSS 3.x – High (7.5) CVSS 2.0 – Medium (5.0)	Обновление версии mysql до 4.41.0

	отказ в обслуживании (сбой) с помощью векторов, связанных с сообщением об ошибке.		
CVE-2011-3599	Модуль Crypt::DSA (он же Crypt-DSA) 1.17 и более ранних версий для Perl, когда /dev/random отсутствует, использует модуль Data::Random, который облегчает удаленным злоумышленникам подделку подписи или определение ключа подписи подписанного сообщения с помощью брутфорса.	CVSS 3.x – not available CVSS 2.0 – Medium (5.8)	Исправлено в версии: perl-Crypt-DSA-1.17-10.*, perl-Crypt-DSA-0.14-8.el5
CVE-2011-2201	Модуль Data::FormValidator 4.66 и более ранних версий для Perl, когда включен параметр untaint_all_constraints, неправильно сохраняет атрибут заражения данных, что может позволить удаленным злоумышленникам обойти механизм защиты от заражения через ввод формы.	CVSS 3.x – not available CVSS 2.0 – Medium (4.3)	Исправлено в версиях libdata-formvalidator-perl/4.66-3, libdata-formvalidator-perl/4.66-1+squeeze1
CVE-2010-1168	Safe (он же Safe.pm) модуль до 2.25 для Perl позволяет контекстно-зависимым злоумышленникам обходить предполагаемые (1) ограничения доступа Safe::reval и (2) Safe::rdo, а также вводить и выполнять произвольный код с помощью векторов, включающих неявно вызываемые методы и неявно благословленные объекты, как продемонстрировано методы (a) DESTROY и (b) AUTOLOAD, относящиеся к "автоматическим методам".	CVSS 3.x – not available CVSS 2.0 – High (7.5)	Обновитесь до Safe.pm версия v2.25 или выше.
CVE-2009-1884	Случайная ошибка в функции bzip2 в Bzip2.xs в модуле Compress-Raw-Bzip2 до версии 2.018 для Perl позволяет	CVSS 3.x – not available CVSS 2.0 –	Исправлена в версии perl-Compress-

	контекстно-зависимым злоумышленникам вызывать отказ в обслуживании (зависание или сбой приложения) через созданный сжатый поток bzip2, который вызывает переполнение буфера, что является проблемой, связанной с CVE-2009-1391.	Medium (4.3)	Raw-Bzip2 2.0.18
CVE-2009-0663	Переполнение буфера на основе кучи в модуле 1.49 DBD::Pg (он же DBD-Pg или libdbd-pg-perl) для Perl может позволить контекстно-зависимым злоумышленникам выполнять произвольный код через неопределенный ввод в приложение, которое использует функции getline и pg_getline для чтения строк базы данных.	CVSS 3.x – not available CVSS 2.0 – High (7.5)	Исправлена в версии 1.50 DBD::Pg